Abstract

A data pipeline is secured in a computer system for the delivery of secure, confidential or proprietary content such as audio, video, software, copyrighted media, etc. A third party application seeks authentication information in connection with a request to deliver data to a unique medium. The system includes driver software of a host as an interface between a storage device and the third party software application, the storage device and the unique medium. The system enables authentication of the link between the third party application and the driver software by providing third party application developers a toolkit or API for interacting with the driver software. The toolkit includes means to request and decrypt an encrypted driver software digital signature previously generated based on the host's driver software and to compare the digital signature with a second digital signature generated at runtime based on the host's driver software. The third party application has access to the public key of a public/private asymmetric key pair, and the driver software is hashed and encrypted with the private key, which remains secret, to form the encrypted driver software digital signature. If a match or correlation is made based on the comparison, the link is secure and the driver software is authenticated, making way for a secure delivery of the serial number of the unique medium to the third party application.